(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号

特表平8－507619

(43)公表日　平成８年(1996)８月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		
Ｇ０９Ｃ	1/00		7259－5Ｊ			
Ｈ０４Ｌ	9/06					
	9/14					
			8842－5Ｊ	Ｈ０４Ｌ	9／00	Ａ
			8842－5Ｊ		9／02	Ｚ

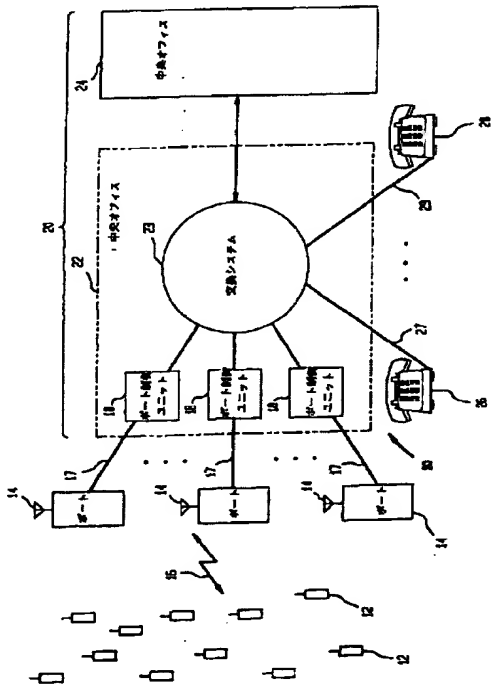
審査請求　有　　予備審査請求　有　（全 30 頁）　最終頁に続く

(21)出願番号　特願平6－520043
(86)(22)出願日　平成６年(1994)２月25日
(85)翻訳文提出日　平成７年(1995)８月23日
(86)国際出願番号　ＰＣＴ／ＵＳ９４／０１９６８
(87)国際公開番号　ＷＯ９４／２１０６７
(87)国際公開日　平成６年(1994)９月15日
(31)優先権主張番号　０８／０２６，６７３
(32)優先日　1993年３月４日
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＪＰ

(71)出願人　ベル　コミュニケーションズ　リサーチ　インコーポレーテッド
アメリカ合衆国、07039―2729　ニュージャージー州、リビングストン、ウエスト　マウント　プレザント　アベニュー　290
(72)発明者　ベラー、マイケル、ジョナサン
アメリカ合衆国、07739　ニュージャージー州、リトル　シルバー、ジュディス　ロード　37
(72)発明者　ヤコビ、ヤコブ
アメリカ合衆国、07922　ニュージャージー州、バークレイハイツ、ルトガーズ　アベニュー　95
(74)代理人　弁理士　小林　孝次

(54)【発明の名称】　低価格端末装置のための二方向公開キー確証およびキー一致

(57)【要約】
最低限の計算リソースを有する第1当事者（12）と、証書認証およびキー分布のためのモジュラー平方根動作、およびElGamal、NIST、DSS、またはメッセージの署名を取得するための他の有効な署名動作を使用する相当の計算リソースを有する第2当事者（18）の間での相互認証およびセッションキー一致の達成する方法。第2当事者（18）は中央オフィス（22）にある交換システム（23）に接続される。



【特許請求の範囲】

請求項1　通信セッションの開始時に、端末装置とサーバの間で相互識別とセッションキー一致を行なう方法で、下記のステップからなるもの

（a）　サーバから端末装置へ、サーバの識別、サーバの公開キーN_j、およびサーバの証書C_jを送信するステップで、これが有効である場合$\sqrt{h}(j, N_j) \bmod N_u$と合同であるもの

で、式中N_jはサーバの公開キー、N_uは中央オーソリティの公開キー、h（　）は一方向ハッシュ機能を示すもの、

(b)　端末装置において、受信した証書C_jが$h(J, N_j)\, C_j^2 \bmod N_u$を満足することを検証するステップ、

（c）　端末装置において、ランダム数x＝（x_L, x_R）を選択し、$y = x^2 \bmod N_j$を得て、yを該サーバに送信するステップ、

（d）　該サーバにおいて、$N_j = p_j q_j$となるように、p_j q_jというサーバの秘密キーを利用することにより、$y = (x_L, x_R) \equiv \sqrt{y} \bmod N_j$を得るために、モジュラー平方根動作を実施し、$x_L$を端末装置に戻るように送信するステップ、

（e）　セッションキーとしてx_Rを使用して暗号化された形で端末装置の識別i、端末装置の公開キーp、および端末装置の証書c_i（これが有効である場合、$\sqrt{h}(i, P_i) \bmod N_u$と合同）を端末装置からサーバに送信するステップ、

(f)　サーバにおいて、受信した証書c_iが$h(i, P_i) \equiv c_i^2 \bmod N_u$を満足することを検証するステップ、

（g）　端末装置において、メッセージmに非対称的署名動作を適用することによってネットワークが送ってきたチャレンジm上で署名s（m）を計算し、x_Rをセ

ッションキーとして使用し、署名を暗号化した形でサーバに送信するステップ、および

（ｈ）　署名動作を逆転することによって、サーバで署名を検証するステップ。

請求項2　　請求項1記載の方法で、該署名S（ｍ）が順序対（ｖ，ｗ）で表され、その対において、

$$P_i^{v} v^{w} \equiv \alpha^{m} \bmod N_s$$

となり、式中、

P_iは該端末装置の公開キー、

N_sは署名法であり、これが素数または2つの素数の積、

αは、整数法N_s，$Z^{**}_{N_s}$の乗法群の最大巡回部分群の中の生成元であるもの。

請求項3　　請求項2記載の方法で、該メッセージm上で署名S（ｍ）を評価するステップが

$$w = (m - s_i v) \cdot r^{-1} \bmod \phi(N_s)$$

という実時間動作を実行し、式中rは事前決定された数、はφ（Ｎ）はオイラーのトーシェエント関数、およびgcd（ｒ，φ（Ｎ））＝1であるもの。

請求項4　　請求項3記載の方法で、端末装置が署名を評価するごとにrの値が個別に選択されるもの。

請求項5　　請求項1記載の方法で、該署名動作がElGamal署名動作であるもの。

請求項6　　請求項1記載の方法で、該著名S（ｍ）が、国家標準局および技術ディジタル署名規格アルゴリズムに従って計算されたもの。

請求項7　　請求項1記載の方法で、該端末装置で受信した証書c_jが$c_j^2 \bmod N_u = h(j, N_j)$という式を満足しない場合、該通信セッションが中止されるもの。

請求項8　請求項1記載の方法で、該サーバで受信した証書 c_j が $c_j^2 \bmod N_u = h(i, P_j)$ という式を満足しない場合、該通信セッションが中止されるもの。

請求項9　請求項1記載の方法で、該端末装置が携帯型通信システムであり、該サーバは該携帯型通信システムのポート制御ユニットであるもの。

請求項10　請求項9記載の方法で、該端末装置が携帯電話であるもの。

請求項11　請求項1記載の方法で、端末装置がスマートカードであり、サーバがスマートカードのベースユニットであるもの。

請求項12　請求項1記載の方法で、端末装置がアナログディスプレイサービスインターフェース（ADSI）端末装置であり、該サーバがADSIのネットワーク暗号サーバであるもの。

請求項13　請求項1記載の方法で、該端末装置が計算上虚弱であり、該サーバが計算上強靭であるもの。

請求項14　請求項1記載の方法で、通信セッションを行なう前に該サーバは、サーバのためにその p_j , q_j および公開キー $N_j = p_j q_j$ 選択し、公開キー N_j を中央オーソリティ

に送信し、証書 c_j を中央オーソリティに置いて形成して証書 c_j をサーバに送信し、該公開キー N_u を該中央オーソリティから該サーバへ送信し、キー N_u を該サーバにおいて記憶することによって初期化されるもの。

請求項15　請求項13記載の方法で、該初期化ステップが該秘密キー S_i を選択し、対応する公開キー P_i を生成し、証書 c_i を中央オーソリティにおいて形成し、証書 c_i を端末装置に送信し、中央オーソリティの公開キー N_u を端末装置に送信することからさらになるもの。

請求項16　請求項3記載の方法で、端末装置iが別の署名法 N_S を有するもので、
端末装置 i の証書が $c_i = \sqrt{h(i) P_i, N_S} \bmod N_u$ の形であるもの。

請求項17　請求項1記載の方法で、該ランダム数 x は、該サーバが $\sqrt{y} \bmod N_j$ を計

算するとき該サーバが適切な根を識別することができるように該端末装置において色付けになっているもの。

請求項18　サーバと端末装置の間で相互確証とセッションキー一致を行なう方法で、下記のステップからなるもの

(a)　該サーバから該端末装置に該サーバの証書を送信するステップ、

(b)　該端末装置において該サーバの該証書の確証性を検証するステップ、

(c)　該端末装置でランダム数xを選択することによって該端末装置とサーバにセッションキーを分布し、該端末装置において該サーバの秘密キーの知識を有することのみによって逆転できる非対称的キー動作を実施することにより、該端末装置において該数xを暗号化するステップ、

(d)　該端末装置から該サーバに暗号化形態で該数xを送信し、該サーバにおいてxを得るように該サーバの該秘密キーを使用することによって該動作を逆転するステップ、

(e)　該数xに依存するセッションキーを使用して暗号化した該端末装置の証書を、該端末装置から該サーバに送信するステップ、

(f)　該サーバにおいて、該端末装置証書の確証性を検証するステップ、

(g)　非対称的署名動作を使用し、該端末装置においてメッセージmの署名S(m) を評価するステップ、および

(h)　該セッションキーを使用して、暗号化形態で署名を該サーバに送信し、該サーバ

において著名動作を逆転するステップ。

請求項19　請求項18記載の方法で、該ステップ(a) が該サーバの識別**j、該サーバの公開キーN_j、および証書c_jを該サーバから該端末装置に送信するものからなるもの

で、これが有効である場合$c_j \equiv \sqrt{h(j, N_j)} \bmod N_u$の形態であり、式中$N_u$は中央オーソリティの公開キーであるもの。

請求項20　請求項19記載の方法で、該ステップ(b)は$h(j, N_j) \equiv c_i^2 \bmod N_u$か否か

を決定するもの。

請求項21　請求項18記載の方法で、該非対称的公開キー動作が$y \equiv x^2 \bmod N_j$であるもので、式中N_jはサーバの公開キーであるもの。

請求項22　請求項21記載の方法で、$x=(x_L, x_R)$であり、式中x_Rが該セッションキーであり、該サーバが$x^2 \bmod N_j$の適切な根を識別することができるようxが色付けになっているもの。

請求項23　請求項18記載の方法で、該ステップ(e)が、該端末装置の識別i、該端末装置の公開キーPi、および該端末装置の証書ciを送信することからなるもので、これ
が有効である場合、$c_i \equiv \sqrt{h(i, P_i)} \bmod N_u$であるもの。

請求項24　請求項23記載の方法で、ステップ(f)が、$h(i, P_i) \equiv c_i^2 \bmod N_u$であるか

否かを決定することからなるもの。

請求項25　請求項18記載の方法で、該署名動作がElGamal署名動作であるもの。

請求項26　通信セッションの開始時に、第1当事者と第2当事者の間で相互確証とセッションキー一致を行なう方法で、下記のステップからなるもの

(a)　該第1当事者においてランダム数を選択し、非対称的公開キー暗号化動作を用いて該ランダム数を暗号化し、暗号化されたランダム数を第2当事者に送信し、該ランダム数を得るため、該第2当事者において該暗号化動作を逆転することによってセッションキーを該当事者間に分布するステップ、および

(b)　該第1当事者は署名S(m)を得るため、メッセージmに非対称的署名動作を実施し、該署名S(m)を暗号化するため暗号機能および該ランダム数に依存するセッションキーを用い、該第2当事者に暗号化された署名S(m)を送信し、該第2当事者において該署名S(m)を解読し、該署名動作を逆転するステップ。

請求項27　請求項26記載の方法で、該公開キー暗号化動作が、該第1当事

者おいて1回のみのモジュラー乗算を使用し、該ランダム数を平方するステップからなるもの。

請求項28　請求項26記載の方法で、該著名動作が、該第1当事者おいて1回のみの実時間モジュラー乗算を使用するElGamal署名動作であるもの。

請求項29　請求項26記載の方法で、該第1当事者おいて1回のみのモジュラー乗算を実施することによって、該第1当事者おいて該第2当事者の証書を確証するステップからさらになるもの。

請求項30　請求項26記載の方法で、該第2当事者において該第1当事者の証書を確証するステップからさらになるもの。

請求項31　請求項26記載の方法で、該第2当事者が該第1当事者よりも多くの計算上りソースを有するもの。

請求項32　請求項26記載の方法で、該第1当事者が携帯型通信システムであり、第2当事者が携帯型通信システムのポート制御ユニットであるもの。

請求項33　請求項26記載の方法で、該第1当事者が端末装置であり、第2当事者がサーバであるもの。

請求項34　請求項33記載の方法で、該端末装置がスマートカードであり、ザーバがスマートカードのベースユニットであるもの。

請求項35　請求項31記載の方法で、端末装置がアナログディスプレイサービスインターフェース（ADSI）であり、サーバがADSIのネツトワーク暗号サーバであるもの。

請求項36　請求項26記載の方法で、第1当事者がサーバであり、第2当事者が端末装置またはワークステーションであるもの。

請求項37　通信媒体を介して通信する第1当事者と第2当事者の間で相互確証とセッションキー一致を行なう方法で、下記のものからなるもの

（a）　該第2当事者から該第1当事者に該第2当事者の証書を送信するもの、

（b）　該第1当事者において該第2当事者の該証書の確証性を検証するもの、

（c）　該第1当事者でランダム数xを選択することによって該第1当事者と第2当事者にセッションキーを分布し、該第1当事者において該第2当事者の秘密キーの知識を有することのみによって逆転できる非対称的キー動作を実施することに

より、該第1当事者に

おいて該数xを暗号化するもの、

(d)　該第1当事者から該第2当事者に暗号化形態で該数xを送信し、該第2当事者においてxを得るように該サーバの該秘密キーを使用することによって該動作を逆転するステップ、

(e)　該数xに依存するセッションキーを使用して暗号化した該第1当事者の証書を、該第1当事者から該第2当事者に送信するステップ、

(f)　該第2当事者において、該第1当事者証書の確証性を検証するステップ、

(g)　非対称的署名動作を使用し、該第1当事者においてメッセージmの署名S(m) を評価するステップ、および

(h)　該セッションキーを使用して、暗号化形態で署名を該第2当事者に送信し、該第2当事者において署名動作を逆転するステップ。

【 発明の詳細な説明】

発明の名称　低価格端末装置のための二方向公開キー確証およびキー一致

関連出願特許

「 ユーザ確証およびキー一致のための暗号方法」と題された特許出願は、M.J. Beller、L.F.Chang、およびY.Yacobiが1991年11月8日登録、シリアルNo.789,700が発行され、本書の代理人に割り当てられた。上述の出願は、本出頁に関する事項を含んでおり、本書に参考として記載した。

発明の分野

本発明は、公開キー暗号を使用して1組の当事者の間で相互の確証およびセッションキー一致を行なう方法に関する。さらに詳しくは、本発明は、当事者の一方が計算上虚弱(つまり計算性能が最低限) であり、他方の当事者が計算上強靭な(つまり計算性能がはるかに大きい) システムに適用できる。本発明の実施例では、計算上虚弱な当事者が行なうわずか3回の大きな実時間モジュラー乗算を介して、永久的な秘密を交換することなく2つの当事者間で完璧な確証およびセッションキーの一致が達成できる。これに対して、同レベルの防犯で相互的確証およびセッションキー一致を行なうための従来の方法では、計算上虚弱な当事者側で約200回の大きな実時間モジュラー乗算が必要になる。

発明の背景

携帯型通信システムでは、場所を移動しながら呼出しの間に低電力・低価格の携帯型ディジタル無線電話端末装置を運搬する。

携帯型端末装置によっては、ディジタル信号プロセッサを使用し、低ビットレートで音声を符号化するために必要な複雑なアルゴリズムを行なうものもある。他の携帯型端末装置では、音声を低ビットレートで符号化のためのカスタムチップを使用し、信号発生プロトコルや他のさまざまなタスクを取り扱うための低電力マイクロコントローラを備えている。いずれにしても、携帯型端末装置は小さいバッテリーで長時間の動作を行なう必要があり、携帯型端末装置内のすべての信号処理動作を低電力で行なうことが重要になる。従って、携帯型端末装置内で短時間で行なわれる信号処理の複雑さには限界がある。

携帯型通信システムでは、携帯型無線端末装置が、公益電信柱や建物にある靴箱サイズの無線ポートの適切に高密度のマトリックスを介し、ローカル電話交換ネットワークにアクセスする。各ポートは無線モデムを備えている。各ポートは次に、中央オフィスビルなどにあるポート制御ユニットの形でのサーバを介して、電話ネットワーク交換システムに再び接続される。ポート制御ユニットは、携帯型端末装置間の無線リンクでの使用に適するフォーマットと電話ネットワーク交換システムでの使用に適するフォーマットの間の変換を含むさまざまな処理機能を果たす。

携帯型通信システムは、計算上非対称的であると説明することができよう。つまりこれは、各接続が端末装置の形で計算上虚弱な当事者（つまり計算リソースの小さい当事者）と計算上強靭な当事者（つまり計算リソースが大きな当事者）を有することを意味する。故に、このような非対称的なシステムで使用されるアルゴリズムは、できれば計算上も非対称的であることが望ましい。言い換えれば、このアルゴリズムは計算上虚弱な側では最低限の処理のみが必要であり、計算上強靭な側では相当量の処理を行なうということになる。

携帯型通信システムは、携帯型電話端末装置と、無線を介した固定位置ポートのアレイの間での会話を通信するため、携帯型通信システムの会話は有線ネットワークの会話よりも盗聴されやすい。

さらに、特定のネットワーク上の特定ワイヤペアにつながる有線電話とは異なり、携帯型電話端末装置は、場所を移動し、異なるポートを介して異なる時間にネットワークにアクセスする。ユーザと特定の物理的位置の関係が欠如しているため、携帯型通信システムは、サービスを不正に利用されやすい。

本発明は、特にメッセージ暗号化（つまり会話内容の暗号化）、キー一致および分布（メッセージ暗号化技術に必要なキー分布）、および確証（つまりサービスの要請が合法であること）に関するものである。さらに詳しくは本発明は、盗聴者（つまり無線機器を使用して携帯端末装置とポートの間の無線通信を傍受する者）を食い止めることに関するものである。

携帯型通信システムを特長づけるもう一つの問題として、ユーザの追跡可能度の問題がある。具体的に説明すると、ユーザが識別情報をクリアで通信すると、

盗聴者がユー

ザの所在地を発見することでき、ユーザの所在地に関するプライバシーが維持できなくなるという点である。本発明はユーザの所在地のプライバシーを維持することに関するものでもある。

盗聴はメッセージ暗号化技術の使用により防止することができる。メッセージ暗号化技術は、データ（会話内容など）を暗号化するセッションキーと呼ばれる数字を用いる暗号化関数を使用する。特定の会話で、携帯型端末装置、および携帯型端末装置が通信状態にある特定のポート制御ユニットは、正しい携帯型端末装置とポート制御ユニットのみがディジタル信号の暗号・解読ができるよう、セッションキーを知るべきである。暗号化関数の2つの例としては、国家標準局の「データ暗号化基準」（DES）（国家標準局「データ暗号化基準」[Data Encryption Standard]、FIPS-PUB-45、1977年などを参照）およびさらに近年の「迅速な暗号化アルゴリズム（FEAL）（ShimizuおよびS.Miyaguchiによる「FEAL--迅速なデータ暗号化アルゴリズム」[FEAL-FastData Encipherment Algorithm]、Systems and Computers in Japan、第19巻、第7号、1988年、およびS.Miyaguchiによる「FEAL暗号系」、CRYPTO '90議事録、カリフォルニア州サンタバーバラ、1990年などを参照）がある。暗号化関数を使用する一つの方法は、電子コードブック技術である。この技術では、単純テキストメッセージmが暗号化され、公式c＝f(m,sk)による暗号化関数fを使用して暗号化テキストcが生成される。式中、skはセッションキーである。暗号化テキストメッセージcはセッションキーskを知っている場合のみ解読でき、単純テキストメッセージ$m=f^{1}(c,sk)$を得ることができる。

携帯型通信システムでDESやFEALのような暗号化機能を使用する場合の一つの問題は、セッションキーの一致である。

従来のセッションキー一致技術では、各携帯型端末装置iはそれのみが知る秘密キーk_iと暗号データベースDBを有する。同様に、各ポート制御ユニットjは、それのみが知る秘密キーk_jおよび暗号データベースDBを有する。通信セッションの開始時点で、携帯型端末装置iはサービスの要請およびその識別iをクリアでポ

ート制御ユニットjに送信する。ポート制御ユニットは、その組(i,j)を暗号データベースDBに送信する。DBはランダムセッションキーskを選び、ポート制御ユニットjに送信する組c_i,c_jを生成する。式中、c_i＝f(k_i,sk)およびcj＝f(k_j,sk)である。ポート制御ユニットjはc_jを解読してskを

見つけ、c_iを携帯型端末装置iに送る。携帯型端末装置iはc_iを解読してskを見つける。

ここでポート制御ユニットjおよび携帯型端末iは両方ともセッションキーskをもっている。故に、暗号化されたメッセージc＝f(m,sk)は、携帯型端末装置iとポート制御ユニットjの間を行き来して送信される。

この方法にはいくつかの利点がある。まずこの方法では、携帯型端末装置側で従来型の暗号化のみを使用するため、同装置での電力は最低限でよいという点である。特に、f およびf⁻¹を評価するために必要な計算能力はかなり小さい。

さらに携帯電話iのふりをする携帯電話は、秘密であるはずのキーkiを事前に知っている必要があるため、従来型キー分布の方法も自己確証的である。

これに対して、従来型キー分布プロトコルは秘密暗号化キーのデータベースを必要とし、これは保護や維持が困難なうえ、システムの存続と信頼性の問題を起こすものである。最大の弱点は、可能な盗聴者がひとたび携帯電話iのためのキーk_iを入手できると、iが知らないうちに続けてiのすべての会話を傍受することができる点である。これは発生する最悪の損害であり、検知不可能なプライバシーの侵害である。また、従来型のキー分布プロトコルには追跡可能度の問題もある。携帯型端末装置は、セッションキーをデータベースから取り込む前に、その身元をクリアで表明しなければならない。従って、盗聴者は特定の携帯端末装置の所在地を見つけだすことができる。

携帯型通信システムでのセッションキー分布と当事者確証に対するもう一つの方法は、公開キー暗号化技術を使用するものである。典型的な公開キー暗号化システムでは、各当事者iは公開キーP_iと秘密キーS_iを有する。公開キーP_iは誰でも知っているものだが、秘密キーはS_iは当事者iのみが知る。ユーザiへのメッセージmは、誰もが知っている公開キーを使用する公開動作を用いて暗号化される

。つまり、c=P(m,P,) であり、式中、cは暗号化メッセージ、mはクリアテキストメッセージ、P_i は公開キー、p は公開動作を示す。しかしながら、このメッセージは秘密キー、つまりm＝S(c,S,) を使用する動作を使用して解読される（式中、s は動作を示す）。秘密キーS_i を有する当事者のみが、暗号化されたメッセージを解読することができるものである。

公開キー暗号化技術は、携帯型通信システムの当事者に対してセッションキーの分布に使用することができる。（上述の米国特許出願、シリアルNo.789,700を参照）。また

公開キー暗号化技術は、携帯型通信システムにおける当事者確証にも使用できる。

確証のための公開キー暗号化を使用する方法の一つとして、署名システムを用いるものがある。P(S(m,S_i) ,P_i) ＝mが真であるとすると、対応キーP_i 、S_i の所有者は、c＝S(m,S_i) を生成することによってメッセージmを署名することができる。mとcが既知であるとすると、ベリファイヤはm＝P(c,P,) であることを確認する。署名システムは、下記のように使用して検証ができる：当事者iの公開キーがP_i であることが周知である場合、かつ他の当事者が自分がiであることを主張した場合、自分がiであることを主張している当事者にメッセージmを用いてそれが正しいか証明するよう要請し、その当事者に秘密キーS_i を使用してメッセージに署名してもらい、次にP_i を用いて署名を検証する。

当事者確証のもう一つの問題は、当事者の公開キーP_i に関する。iと主張するユーザは、公開キーがネットワーク管理者などの信頼されている中央オーソリティによって認証されている限りにおいて、その公開キーを供給することができる。信頼されている中央オーソリティ自体は周知の公開キーP_u である。証書とは、ユーザの身元iとその公開キーP_i 間の信頼されているオーソリティの署名である。

セッションキー分布のための最高レベルの防犯、および公開キー暗号化をもとにした当事者相互確証は下記のことを行なう：

1）秘密情報のオンライン中央データベースの使用を避ける、

2) 盗聴者からユーザの身元を隠す、

3) 当事者の間で、永久的秘密を交換しないような方法で、相互的確証およびセッションキー一致を行なう。

最もよく知られている公開キーアルゴリズムであるRSAを用いて最高レベルの防犯を行なうには(例えばR.L.Rivest、A.Shamir、L.Adlemanによる「デイジタル署名および公開キー暗号システムを得る方法」(A Mcthod for Obtaining Digital Signaturcs and Public-Key Cryptosystems) 、Communications of ACM, 第21巻、第2号、pp.120-126、1978年2月などを参照) 、各当事者が約200回の大きなモジュール乗算を行なわなければならない(この数字は長さが500ビット以上になる) 。上述の米国特許出願シリアルNo.789,700に記載したアルゴリズムを使用すると、この最高レベルの防犯は約200回のモジュ

ール乗算が必要になる。

このような従来技術でのアルゴリズムでの問題は、両当事者側で大量の計算が必要な点である。このことは、一方(例えば端末装置や携帯電話) の計算リソースが虚弱であり、他方(例えばサーバやポート制御ユニット) の計算リソースが強靭であるような非対称的システムには向いていない。従来技術のアルゴリズムは、虚弱側でわずかな量の計算しか必要のないような非対称に十分なっていない。

従って本発明の目的は、一方が計算上虚弱であり他方が計算上強靭である非対称的システムにおいて、高レベルの防犯でキー分布と当事者相互確証のための公開キーを暗号化する方法を提供することにある。

発明の概要

本発明は、第1当事者が計算上虚弱(つまり計算リソースの限られた当事者) であり、第2当事者が計算上強靭な当事者(つまり計算リソースが大きな当事者) である2つの当事者間の通信セッションのための相互確証およびセッションキー分布の方法に関する。例えば、第1当事者は携帯電話などの形での端末装置、第2当事者は無線パーソナル通信システムにおけるポート制御ユニットの形でのサーバとすることができる。

本発明によると、2つの高度に非対称的な公開キー暗号化動作を使用する。証書の確証およびセッションキー分布には、モジュラー平方根動作を使用する。ElGamal著名動作（例えばT.ElGamalによる「ディスクリートロガリズムを基礎にした公開キー暗号システムおよび署名構造」（APublic Key Cryptosystcm and Signature Scheme Based on Discrete Logarithms）、IEEET rans.IT、第IT-31巻、第4号、1985年7月、pp.469-472などを参照）は、計算上虚弱な当事者側の署名を得て検証するために使用される。これらの動作を使用する場合では、すべての相互確証およびセッションキー分布法に、計算上虚弱な当事者側でわずか3回の実時間モジュラー乗算が必要なだけである。モジュラー平方根およびElGamal動作は、上述した非対称的システムに極めて適している。これらは実時間計算能力をほとんど必要しない暗号化動作を使用するが、これは計算上虚弱な側で実施することができ、相当の計算能力を必要とする逆解読動作は計算上強靭な当事者側で実施できる。

本発明の実施例に従うと、最初の段階で、サーバの公開キー（計算上強靭な側）およ

びサーバの証書は、端末装置（計算上虚弱な側）に送信される。そこでサーバの証書が検証される。ランダム数$x=(x_L, x_R)$が端末装置で選ばれ（式中、(x_L, x_R)は、2つの数x_Lおよびx_Rを示す）、モジュールとしてのサーバの公開キーを使用してxを平方することにより暗号化される。

M.O.Rabinによる「因数分解のように加工不可能なディジタル化署名および公開キー関数」（Digitalized Signature and Public Key Functions as Intractable as Factorization）、MITLaboratory for Computer Science、TR212、1979年1月）。その結果はサーバに送信され、サーバはその秘密キーを用いて平方動作を逆転する。従って、両側はxを有する。故に、xまたはx_Lまたはx_Rをセッションキーとして使用することができる。数x_Lまたはx_Rはサーバから端末装置に送信されて戻され、そのサーバが事実xを得ることができたことを検証することができる。後の段階で、端末装置の公開キーおよび端末装置の証書は、セッションキーを用いて従来の方法で暗号化されたサーバに送られる。この端末装置は、サー

バで検証される。ネットワークからの証明要請のElGamal署名は、端末装置で計算され、セッションキーを用いて従来の方法で暗号化され、サーバに送信される。ElGamal署名動作は、端末装置の以前に送信された公開キーを用いてサーバで逆転され、署名を検証する。もう一つの実施例では、ElGamal構造の代わりに、全米技術規格協会（NIST）のディジタル署名規格（DSS）アルゴリズムを署名構造として使用することができる。さらに別の実施例では、ElGamal構造の代わりに、著名者のために効果的な署名システムを使用できる。例えば：Even GoldreichおよびMicali（S.Even、O.Goldreich、S.Micaliによる「オンライン／オフラインのディジタル署名構造」［On-Linc/Off-Linc Digiml Signature Schcmcs］、Advances in Cryptology-CRYPTO '89議事録、G.Brassard編、Lecture Notes in Computer Scicnce、第435巻、Springer-Vedag、1990年、pp.263-275）、Schnorr（C.P.Schnorrによる「スマートカードによる効果的な署名生成」［Efficient Signature Generation by SmartCards］、Joumal of Cryptology、第4巻、第3号、1991年、pp.161-174）、Shamir（A.Shamirによる「置換え済み中核を基礎にした効果的識別構造―長抄録」［An Efficient Identification Scheme Based on Pcrmuted Kemels-Extended Abstract］、CRYPtO'89議事録、G.Brassard編、LNCS 435、pp.606-609）、またはFiatおよびShamir（A.Fiat、A.Shamirによる「自分を証明する方法：識別および署名における問題の実用的解決方法」

［How to Prove Yourself:Practical Solution to Idcntification and Signature Problems］、CRYPTO'89議事録、A.M.Odlyzko編、LNCS 263、1987年、pp.186-194）などのシステムが使用可能である。

本発明の方法には、虚弱側当事者で計算上リソースが非常に少なくてすむことに加えて、他にもいくつかの利点がある。本発明の個別要素（実施例でのモジュラー平方根およびElGamal署名）は、第2段階で送信を暗号化するため第1段階で得たセッションキーを用いることによって分離できなくし、よって「中断」攻撃の可能性を防ぐ。さらに無線パーソナル通信システムでは、本発明の方法は、盗聴者に対する防犯を提供し、ユーザの所在地のプライバシーを提供する。個別ユーザの永久的秘密をネットワークに開示する必要はなく、盗聴されやすいオンラ

インデータベースに秘密情報を記憶しておく必要もない。

本発明は主に、携帯型通信システムに関して記載したものであり、さらに詳しくは、携帯型端末装置が携帯電話である携帯型通信システムに関する。但し、この携帯型端末装置は、携帯型通信システムにデータを送信し、同システムからデータを受信する携帯型コンピュータや携帯型ファックス機器、その他の装置である可能性がある点に留意されたい。

概して本発明は、暗号化および当事者相互確証のためのセッションキー分布が必要な環境において、端末装置とサーバが互いに通信するようなシステムに適用される。本発明は特に、端末装置の計算上リソースがサーバの計算上リソースよりはるかに小さい場合に適用される。例えば、端末装置（つまり虚弱側の当事者）はスマートカードで、サーバ（強靭側の当事者）はスマートカードのベースユニットとすることもできる。また、端末装置は、例えば自宅で銀行手続きを行なうために使用するアナログディスプレイサービスインターフェース（ADSI）端末装置が使用でき、サーバはADSI暗号サーバとすることもできる。もう一つの適用法として、多数のクライアントのコンピュータが1つのサーバにアクセスするコンピュータのクライアント／サーバシステムが考えられる。このようなクライアントとサーバは近似した計算能力をもつ可能住がある。この場合では、「虚弱側」の計算をサーバで行ない、計算の負担の均衡をとる方がよいこともある。

図面の簡単な説明

図1は、携帯型通信システムを概略的に図示したもの。

図2は、本発明の実施例に従ったセッションキー分布および当事者相互確証プロトコルを概略的に図示したもの。

発明の詳細な説明

本発明の詳細な説明は次のセクションに分かれている。セクションAは携帯型通信システムについて説明する。セクションBはRabinモジュラー平方根公開キー動作について説明する。セクションCはElGamal署名動作について説明する。セクションDは公開キー証書について説明する。セクションEは、本発明の実施例に従ったセッションキー分布および相互確証プロトコルを説明したものである

。

Ａ．携帯型通信システム

携帯型通信システム10を図1に概略的に図示した。システム10は、複数の低電力、低価格携帯型ディジタル無線端末装置12からなる。携帯型端末12は、ユーザによって色々な場所に移される。ここでは端末装置12は携帯電話にしている。

携帯型端末装置12は、ローカル交換電話システム20と通信を行なう。このローカル交換電話システム20は、中央オフィス22、中央オフィス24、およびライン27と29で中央オフィス22につながった顧客施設内機器26と28によって図1に示した。

上述したように、携帯電話によってはディジタル信号プロセッサ（DSP）を用いるものもあり、音声を低ビットレートで符号化するために必要な複雑なアルゴリズムを実施することができる。また他の携帯電話では、音声を低ビットレートで符号化するためのカスタムチップを使用し、信号プロトコルやその他のさまざまなタスクを取り扱うための低電力汎用マイクロコントローラを備えるものもある。いずれにしても、携帯電話や他の携帯型端末装置は、小さなバッテリーで長時間の動作を行なわねばならず、携帯型端末装置内のすべての信号処理の動作を低電力で行なうことが重要である。

携帯型端末装置12は、ポート14を介してローカル交換電話システム20にアクセスする。特定の携帯型端末装置12および特定のポート14は無線リンクを介して通信する。これを図1の矢印16で概略的に示した。ポート14は一般的に靴箱サイズのもので、公益電信柱や建物に位置する。ポート14のそれぞれはシンプルな無線モデムからなる。

ポート14は、ライン17、およびサーバまたはポート制御ユニット18を介してローカル

交換電話システム20に戻って接続する。ポート制御ユニット18は一般的に中央オフィスビルにあり、さまざまな信号処理機能を果たす。具体的には、ポート制御ユニット18は、無線リンク16を介する通信に適したフォーマットと中央オフィス22の交換システム23での使用に適したフォーマットの間での翻訳を行なう。また

各ポート制御ユニット18は、無線リンク16上でトランスコーディングおよびメッセージの解読に必要な信号処理を実施する。

B．Rabinモジュラー平方根の動作

pおよびqは2つの秘密素数で、N＝pqとする。各ユーザは一組の秘密キーおよび公開キーを有し、公開キーは例えばN以上の複合数、秘密キーはその因数分解pおよびqである。上記のキーの所有者に送るためメッセージxを解読するため、下記の計算を行なう。

$$y = x^2 \bmod N \qquad (1)$$

つまり、単なる1回の大きな乗算である。yとNが既知の場合、xを計算することはNを因数分解することと同様に難しく、従って秘密素数pとqが知られていない限り困難なタスクである。

y、p、qが既知の場合、xを導きだすのは簡単である（約200回の乗算に対応する）。具体的には、素数pとqは、$p \equiv q \equiv 3 \bmod 4$であり、$x = x_p \bmod p$および$x = x_q \bmod q$を導きだすように素数pおよびqを使用する。フェルマーの小定理を使用すると、

$$x_p \equiv y^{(p+1)/4} \bmod p、および x_q \equiv y^{(q+1)/4} \bmod q \qquad (2)$$

の場合

$$x_p^2 \equiv y \bmod p \qquad (3)$$

$$x_q^2 \equiv y \bmod q \qquad (4)$$

となることが容易に分かる。このことから、中国式剰余法を使用して、

$$x \equiv x_p \cdot q \cdot q_i + x_q \cdot p \cdot p_i \bmod pq \qquad (5)$$

と計算することができる。式中のq_iおよびp_iは、

$$q_i \equiv q^{-1} \bmod p、および p_i \equiv p^{-1} \bmod q$$

となるように選択した。　　(6)

x_pが(3)に対する解である場合、$-x_p \bmod p$もそうなるため、解読のためのこの技術の

使用には曖昧さがある点に留意されたい。同様に、x_qが(3)に対する解である

場合、$-x_q \bmod q$もそうなる。故に、合同式（１）には4つの解がある。この曖昧さを解決するため、事前に取り決めたパターンを含むように送信者がxを選択する。次に、解読する当事者側はこの「色付けされた」解を選択する。例えば、xが最も重要でない30ビットですべて0を含む場合、この曖昧さが残るほぼ10億の確率があり、この場合プロトコルは単に中止となって再実行することになる。

ここで使用したように、yが既知の場合に方程式（１）のxを解く上記の手順は下記のように表される。

$$x \equiv \sqrt{y} \bmod N \qquad (7)$$

この技術は、偽造不可能な署名を生成するためにも利用できる。メッセージmに署名を作成するため、広く周知の公開キーN（秘密素数pおよびqの積）を有するユーザは、上記の手順に従って秘密キーpおよびqを用い、署名sを、

$$x \equiv \sqrt{m} \bmod N \qquad (8)$$

のように計算することができる。この署名を検証したい当事者は、上記の合同式が真であるか否かを確かめるだけでよい。この検証には、1回のモジュラー乗算を要するのみである。これに対して、潜在的偽造者は秘密キーp およびq 、つまりNの因数を知らなければならないため署名を偽造することは計算上実行不可能である。この署名構造では色付けの必要はないが、Rabin「逆説」の攻撃を防ぐためメッセージには色付けが必要になる（S.Goldwasser、S.Micali、R.L.Rivcstによる「選択されたメッセージへの攻撃を防ぐデイジタル署名構造」［ADigital Signature Scheme Secured Against Chosen Message Attacks］、SIAMJ.On Cpmpt、第17巻、第2号、1988年、pp.281-308）。この攻撃は、被害者が任意の整数のモジュラー平方根を開平するしようとする際、いつでも実行可能になり、その結果を攻撃者に教えてしまうことになる。また被害者はランダムに可能な根の一つを選ばなければならない。つまり「正しい」根が色付けされており、被害者が色付けされた根に戻った場合、攻撃は失敗となる。そうでない場合、この攻撃は被害者のモジュールの効率的な因数分解になる。本発明のプロトコルでは、この攻撃は実行不可能である。

C．ElGamal署名

P_aおよびS_aをユーザaの公開キーおよび秘密キーとする（ここで$P \equiv \alpha^{S_a} \bmod N_s$）。ElGamal署名モジュールの$N_s$は、2つの素数の積の素数でも複合数でもなく、アルファは整数法N_sの乗法群の最大巡回部分群$Z^*_{N_s}$における生成元である（例えば、N.Koblitzによる「数論および暗号におけるコース」［A Course in Number Theory and Cryptogmphy］、Springer Vcrlag、1987年、p.32などを参照）。ユーザaによる、メッセージm上のElGamal署名は順序対（v,w）であり、これは、

$$P_a^v \cdot v^w \equiv \alpha^m \bmod N_s \qquad (9)$$

である。故に、署名の受信者は容易にこれを検証することができる。署名を作成するには、ユーザはランダム数rを選び、$v \equiv \alpha^r \bmod N$を計算する。（9）より、

$$S_a \cdot v + r \cdot w \equiv m \bmod \phi(N) \qquad (10)$$

となり、式中の$\phi(N)$はオイラーのトーシェエント関数である。故に、S_aを知るaは（これを知るのはaのみである）、gcd（r,$\phi(N)$）＝1である場合（gcdは最大公約数を表す）、wを計算することができる。

特定の注意事項を考慮した場合、S_aを知らない者が署名を偽造することは非常に困難であると考えられている。

r、v、r^{-1}および$S_a \cdot v$は事前に準備しておくことができるため（これらは署名するメッセージから独立している）、重要なオンライン（つまり実時間）動作のみが、

$$w \equiv (m - S_a v) \cdot r^{-1} \bmod \phi(N) \qquad (11)$$

において、r^{-1}によって乗算される。

ここで署名者によってランダムに選ばれた値rが、各著名ごとに変更されなければならない点に留意することが重要である。そうでない場合、著名者の秘密S_aが明かされてしまうことになる。

D．公開キー証書

公開キー証書とは、識別とそれに対応する公開キーと主張するもののリンクに

おける信頼の高いオーソリティの署名である。秘密キーp_uと公開キー$N_u = p_u \cdot q_u$を有する中央オーソリティ（CA）がある。この中央オーソリティは、端末装置（例えば携帯型通信ユニット）またはネットワークサーバ（例えばポート制御ユニット）が初期化されたとき、固有の識別iが与えられ、独自の秘密キーp_i、q_i、またはS_iを選択した後、Rabinモジュ

ラー平方根構造に従ったN_i、またはElGamal構造に従ったP_iのいずれかの対応する公開キーを計算する。

次に中央オーソリティは、Rabin構造の場合でのiとN_iの間のリンク（またはElGamalではiおよびP_iの間）において、署名をもった端末装置またはサーバを提供する。リンクは関連するアイテムの連結の一方向ハッシュとなることもある。通信セッションの間、ElGamal公開キーP_iをもつ端末装置は、その識別、公開キー、および証書をネットワークサーバに送信する。サーバによって証書がひとたび検証されるとにの処理は一つの平方法N_uが必要であり、また識別と公開キーの間のリンクにCAが一致したことを証明するものである）、端末装置は、P_iに関連する秘密キーを用いて、ランダムの証明要請メッセージmに対して、その識別を証明することができる。

同様にサーバも、その識別、公開キー、および証書を端末装置に送信することができる。端末装置は、証書法Nuを平方してリンクを確認し、サーバの検証済み公開キーをもつ暗号化されたメッセージを送信することができる。サーバは、公開キーに関連する秘密動作（解読）を実施することによって、その識別を証明することができる。

E．セッションキー分布および相互確証プロトコル

図2は、本発明の実施例に従ったセッションキー分布および相互確証プロトコルを図示したものである。このプロトコルは、計算上虚弱な端末装置（例えば携帯型通信ユニット、ADSI、スマートカードなど）と計算上強靭なサーバ（例えばポート制御ユニット、ADSIネットワーク暗号サーバ、スマートカードベースユニットなど）の間での各通信セッションの開始時に使用することができる。

このプロトコルを使用するには、端末装置とサーバを初期化する。サーバを初

期化する際(図2の(a) の部分) 、Rabin秘密キーp_j 、q_j 、および対応する公開キー$N_j = p_j \cdot q_j$を選択する。対応する公開キーN_jは中央オーソリティuに送信される。中央オーソリティはサーバのために固有の識別jを選ぶ。また中央オーソリテイは、Rabin署名(つまりモジュラー平方根) として示した証書c_jの計算をh(j,N_j) 上で行なう。ここで、hはjからなるリンクのハッシュを表す。つまり、$c_j \equiv \sqrt{h(j, N_j)} \bmod N_u$であり、式中$N_u = p_u q_u$は中央オーソリティの法である。

次に、中央オーソリテイはj、c_j 、α (ElGamal生成元) 、N_s (ElGamal法) 、およびN_u

をサーバjに送信する。するとサーバはj、c_j 、N_j 、α 、N_s 、N_uを記憶する。

端末装置(図2の(b) の部分) を初期化する際、中央オーソリティは固有の識別iを拾い上げ、端末装置に送信する。また中央オーソリティは、α 、N^{**}、およびN_uを端末装置に送信する。端末装置iは秘密キーS_i を選び、上述したElGamal動作に従って関連する公開キーPiを生成する。この公開キーP_i は、中央オーソリティuに送信される。中央オーソリテイuは端末装置iにh(i,P_i) 上でRabin署名(つまりモジュラー平方根) の形

で証書を提供する。つまり$c_j \equiv \sqrt{h(j, p_i)} \bmod N_u$となる。また端末装置iは、中央オーソリティuの公開キーN_uおよびc_i 、S_i 、P_i 、N_sを記憶する。

図2の(c) 部分は、プロトコルにつき1回実施されるが実際のプロトコル実行時間の前に実施する事前計算を示す。事前計算にはElGamal署名動作が必要である。事前計算を実施するためには、端末装置iはランダム数rを選び、$v = \alpha^r \bmod N_s$ 、$r^{-1} \bmod \Phi(N_s)$ 、$S_i v \bmod \Phi(N^{**})$を計算し記憶する。

図2の(d) 部分に示したように通信セッションの開始時で、ネットワークサーバはその識別j、公開キーN_j 、および証書c_jを端末装置に送信する。端末装置は証書c_jを平方することにより、中央オーソリティの公開キーN_uを法として証書c_jを検証する。これが正しい場合、端末装置はランダム数xを拾う。これは2つの半

分x_L、x_R、および「色付け」の連結であると考えられる（例えばoの前にある、または後に続くkで、記号o^kで示される）。次に、端末装置はxを暗号化する。この暗号化には$y=o(x)$の動作を実施するが、できれば単一のモジュラー乗算で実施することが望ましい。例えば、$y=o(x) \equiv x^2 \mod N_j$などである。次に端末装置はyをネットワークサーバに送信する。ネットワークサーバは、$x = o^{-1}(y) \equiv \sqrt{y} \bmod N_j$の動作を実施してyを解読し、正しい「色付け」

の根を選択し、x_Lを端末装置に戻して解読できることにより認証されたネットワークサーバであることを証明する。Rabin「逆説」への攻撃はここでは実行不可能なことに留意されたい。これはサーバが任意の根に応答せず、端末装置が選んだ同一の根（事実、例えばその根のx_Lなど、一部分のみ）を戻すためである。この時点で端末装置とサーバの両方で独占的に知られる数x_Rは、セッションキーとして機能する。

この時点から、プロトコルメッセージ（および続く会話）は、端末装置とサーバの間の通信チャネルにおいて盗聴者から端末装置の身元を隠すため、セッションキーとして

x_Rを用いて会話暗号機能で暗号化される。これは特に携帯電話など、顧客の所在地情報を盗聴者に隠さなければならない場合に有用である。

次に端末装置はその識別i、公開キーP_i、および証書c_iをサーバに送信する。サーバは、中央オーソリティ公開キーを法とし、証書を平方することによってこれを検証する。次に、サーバはランダムの証明要請をメッセージmの形で端末装置に送信する。端末装置は、ランダムの証明要請についてElGamal署名を戻すことによってその識別を証明する。上記に詳述した「事前計算」があらかじめ実施されている場合、署名には実時間モジュラー乗算が1回必要なだけである。次に、サーバはこの署名を検証する。

このプロトコルのバリエーションとして、各端末装置が秘密素因数p_iとq_iを伴う独自の公開ElGamal法N_iを有するものがある。この場合、サーバjが署名動作を逆転するため、N_iはサーバjに送信されなければならない。故に、ここで端

末装置iの証書c_iは、

$c_i \equiv \sqrt{h}(i, P_i) \bmod N_u$ の代わりに $c_i \equiv \sqrt{h}(i, P_i, N_i) \bmod N_u$ の形となる。

このプロトコルのもう一つのバリエーションは、実時間プロトコルの3番目の送信（メッセージx_Lの送信）が排除され、その代わりに同意のパターンまたは「色付け」を有するようチャレンジ（m）が要求されるものである。（キーx_Rでの従来型の暗号を用いて）mを送信メッセージの解読後、当事者iは予想されるパターンが存することを検証する。当事者iは予想されるパターンが存在しない場合、このプロトコルを中止する。これで、端末装置iによるネットワーク側jの認証は完了する。プロトコルの残りは上述したように実施される。

このプロトコルは、完全な公開キー二方向認証およびセッションキー一致を行なう方法で、これは認証プロセスから分離することはできない。これはすべて計算上虚弱な側の3回の大きなオンライン乗算（加えて、数百回の大きなオフライン乗算、および潜在的に約100バイトの追加メモリ）で行なうことができる。これに対して、RSAでは同レベルの防犯を行なうために、両側の数百回大きなオンライン（実時間）乗算が必要である。PCSハンドセットでは、この差は重大である。端末装置でのディジタル信号プロセッサまたは特殊モジュラーべき乗回路のような高性能プロセッサを必要とすることのない優れた実時間性能の提供には、提案されたプロトコルの複雑さが十分に低いため、電力スペースの問題がないADSI端末装置でさえこれは重要と言える。RSAで十分な実時間性

能を発揮するために要求されるこのようなプロセッサは、端末装置のコストを最高$100まで増加させることにもなる。

pcsハンドセットやADSI端末装置に導入されると予想されている8ビットのマイクロコントローラでは、1回のモジュラー乗算に約0.1秒を要する。このプロトコルの分析は、ハンドセットや端末装置が実時間でわずか3回のモジュラー乗算の実施でよいことを示している。これには約0.3秒の処理時間が必要なだけである。（RSAでの約20秒と比較するとよい）ネットワークは計算上強靭であると考えられるため、ネットワーク側での処理時間はほぼ無視できる程度のものと考えて

よい。送信時間はプロトコル実行時間に追加されるが、メッセージによっては組み合わせて送信時間を低下させながら、プロトコルの防犯性を維持したままにできる。

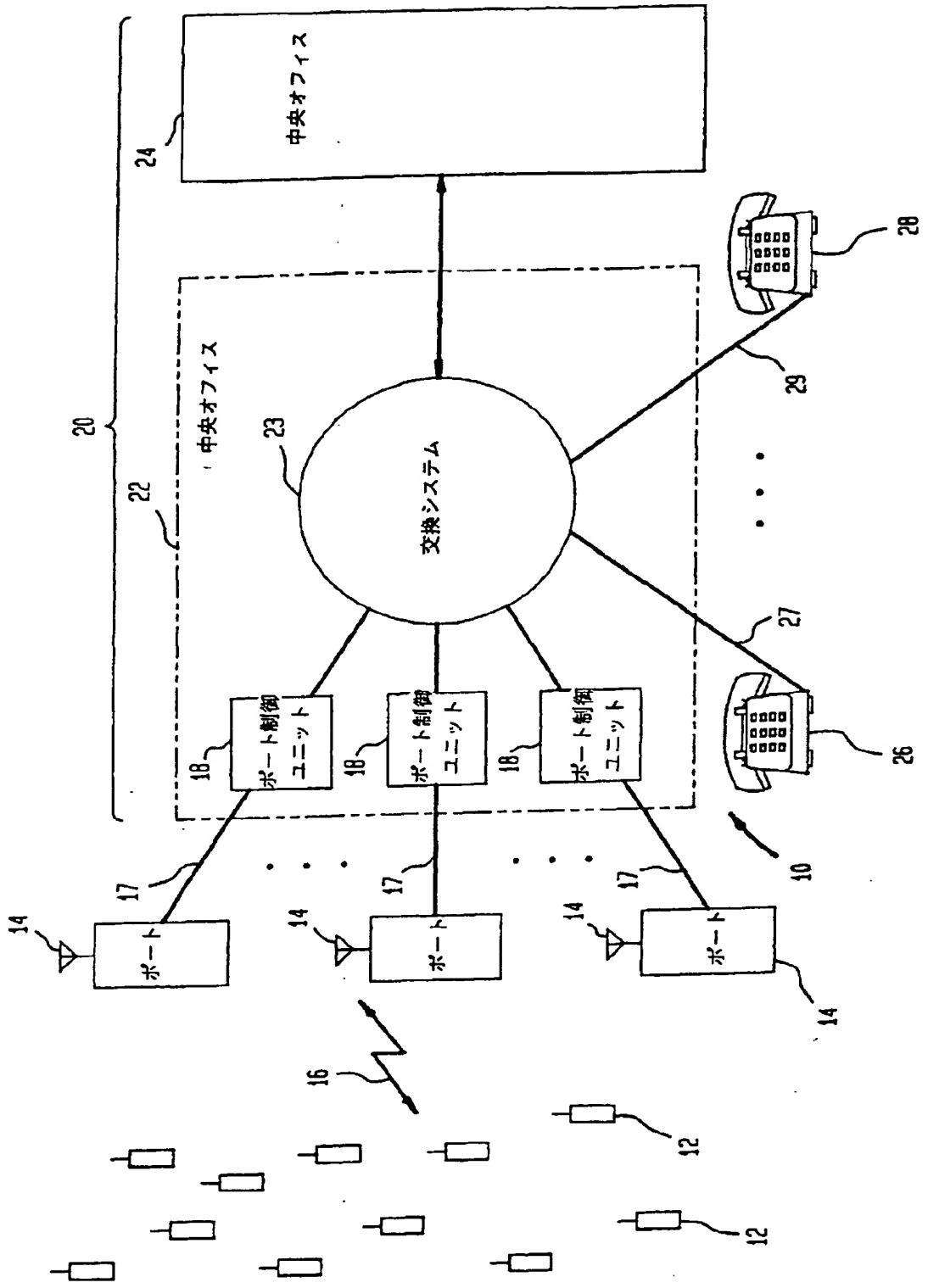
但し、値rを署名ごとに変更しなければならないため、プロトコルの各実行につき約200回の事前モジュラー乗算（8ビットマイクロで20秒）が端末装置において必要である。これは事前に準備しておき、将来のトランザクションのために結果を記憶させておくことができる。

結論

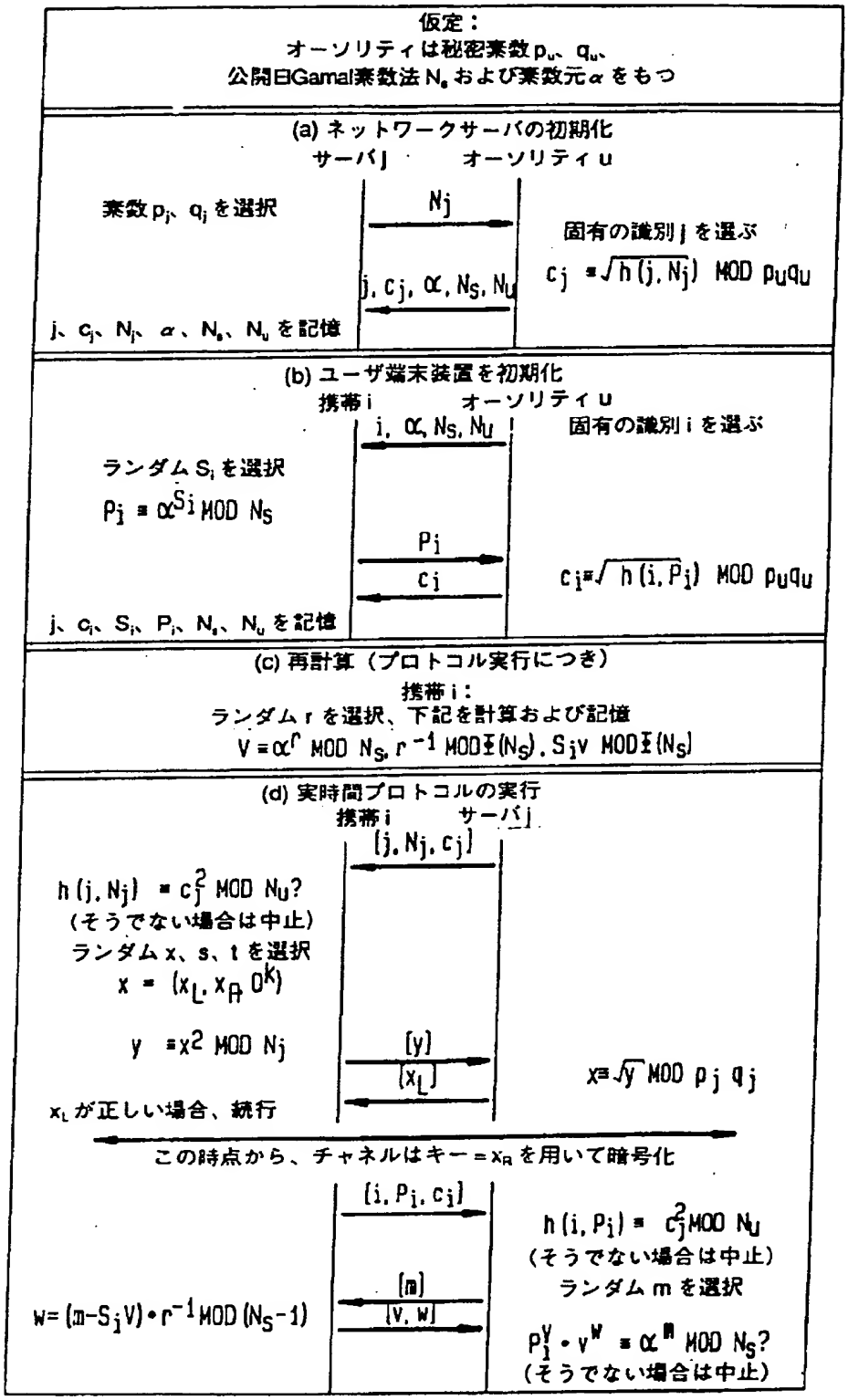
端末装置とサーバの間でのセッションキー一致および相互認証を可能にするプロトコルを開示した。このプロトコルは一方の側で最低限の処理をのみを必要とする。これにより、このプロトコルはPCSハンドセット、ADSI端末装置、およびスマートカードなどに最適である。このプロトコルは、PCSで特に重要な所在地／身元を隠すことができる。

最後に、上述した本発明の実施例は、例としてのみ示したことであることに留意されたい。技術的熟練者であれば、下記の特許請求の範囲から逸脱することなく異なる多くの実施例を作成することができるはずである。

【 図1 】


中央オフィス
24
20
中央オフィス
22
交換システム
23
ポート制御ユニット
18
ポート制御ユニット
18
ポート制御ユニット
18
17
17
17
ポート
14
ポート
14
ポート
14
16
12
12
28
29
27
26
10

【 図2 】


仮定：
オーソリティは秘密素数 p_u、q_u、
公開RGamal素数法 N_u および素数元 α をもつ
(a) ネットワークサーバの初期化
サーバj　　オーソリティu
素数 p_j、q_j を選択
N_j
固有の識別jを選ぶ
$c_j \equiv \sqrt{h(j, N_j)} \bmod p_u q_u$
j, c_j, α, N_S, N_u
j、c_j、N_j、α、N_s、N_u を記憶
(b) ユーザ端末装置を初期化
携帯i　　オーソリティu
i, α, N_S, N_u
固有の識別iを選ぶ
ランダム S_i を選択
$P_j \equiv \alpha^{S_i} \bmod N_S$
P_j
c_j
$c_i \equiv \sqrt{h(i, P_j)} \bmod p_u q_u$
j、c_i、S_i、P_j、N_s、N_u を記憶
(c) 再計算（プロトコル実行につき）
携帯i：
ランダムrを選択、下記を計算および記憶
$V \equiv \alpha^r \bmod N_S$, $r^{-1} \bmod \Xi(N_S)$, $S_j V \bmod \Xi(N_S)$
(d) 実時間プロトコルの実行
携帯i　　サーバj
$[j, N_j, c_j]$
$h(j, N_j) \equiv c_j^2 \bmod N_u$?
（そうでない場合は中止）
ランダム x、s、t を選択
$x = (x_L, x_R\ 0^k)$
$y \equiv x^2 \bmod N_j$
$[y]$
$[x_L]$
$x \equiv \sqrt{y} \bmod p_j q_j$
x_L が正しい場合、続行
この時点から、チャネルはキー $= x_R$ を用いて暗号化
$[i, P_i, c_j]$
$h(i, P_i) \equiv c_j^2 \bmod N_u$
（そうでない場合は中止）
ランダム m を選択
$[m]$
$[V, W]$
$W = (m - S_j V) \cdot r^{-1} \bmod (N_S - 1)$
$P_i^V \cdot V^W \equiv \alpha^m \bmod N_S$?
（そうでない場合は中止）

【 国際調査報告】

INTERNATIONAL SEARCH REPORT

In: tional application No.
PCT/US94/01968

A. CLASSIFICATION OF SUBJECT MATTER
IPC(5) :H04L 9/30
US CL :380/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. 380/21,23,25,30,43,49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,453,074 (WEINSTEIN) 05 JUNE 1984	1-37
A	US, A, 4,723,284 (MUNCK ET AL) 02 FEBRUARY 1988	1-37
A	US, A, 4,799,258 (DAVIES) 17 JANUARY 1989	1-37
A	US, A, 4,876,716 (OKAMOTO) 24 OCTOBER 1989	1-37
A	US, A, 4,935,962 (AUSTIN) 19 JUNE 1990	1-37
A	US, A, 4,969,189 (OHTA ET AL) 06 NOVEMBER 1990	1-37

☐ Further documents are listed in the continuation of Box C.　☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 APRIL 1994	Date of mailing of the international search report 29 APR 1994
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 308-0479

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI
H04L 9/32			